



Transizione alla crittografia post-quantum

Alessandro Casale – Capo Divisione algoritmi e applicazioni
crittografiche

Milano,
22.09.2026



Crittografia Simmetrica

- **Una sola chiave segreta** sia per cifrare che per decifrare
- **Richiede un canale sicuro** per condividere la chiave segreta
- **Algoritmi efficienti**, adatti a processare grandi quantità di dati
- Utilizzi: **cifratura** dati in transito e a riposo
- **Attualmente resistente** alla minaccia quantistica (accorgimenti minimi)



Crittografia a Chiave Pubblica

- **Due chiavi**, una per cifrare (pubblica) e una per decifrare (privata)
- **Non richiede canali sicuri**
- **Schemi inefficienti** per processare grandi quantità di dati
- Utilizzi: **scambio chiave** simmetrica, **firma digitale**
- **Schemi vulnerabili** alla minaccia quantistica (algoritmo di Shor)

Harvest now, decrypt later

Crittografia a Chiave Pubblica

Impiegata in numerosi applicazioni di uso quotidiano quali:

- Servizi Internet (TLS, HTTPS)
- Transazioni finanziarie, home banking e pagamenti online
- Identità digitale, CIE, passaporto
- Firma digitale di documenti
- PEC e posta elettronica sicura
- Aggiornamenti software/firmware
- Smartphone e app
-



Minacciata da algoritmi eseguibili su computer quantistico



Soluzione: individuazione di algoritmi di cifratura resistenti a computer quantistici (*Post-Quantum Cryptography, PQC*)

Schemi post-quantum

Sistemi implementabili sui **computer classici** che si basano su **problemi matematici resistenti** agli attacchi quantistici

SOLUZIONE

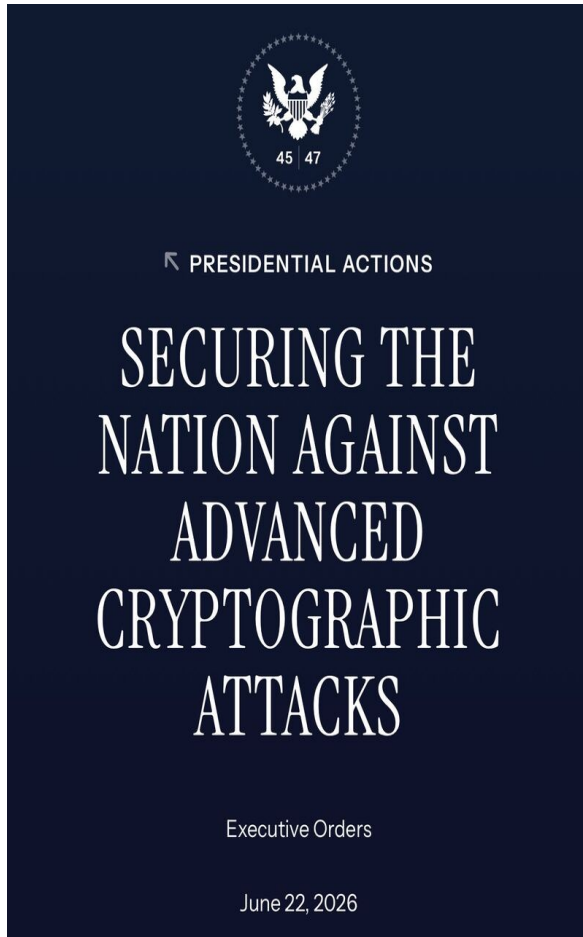
Individuazione di algoritmi di cifratura resistenti a computer quantistici (Post-Quantum Cryptography, PQC)



Contesto	Schemi attuali	Schemi post-quantum
Scambio chiave	RSA DH(E) → ECDH(E)	ML-KEM HQC-KEM
Firma digitale	RSASSA → DSA ECDSA	ML-DSA SLH-DSA LMS/XMSS ...

Transizione alla PQC in USA

Executive Order



22.06.2026

Entro il 22/09/2026 da executive order:

- L'Office Management and Budget deve emanare una *guidance* per la migrazione PQC delle agenzie federali (**emanato il 24 giugno**).



Entro 24/07/2026:

- Ogni Agenzia Federale deve nominare un PQC migration Lead

Entro 22/12/2026:

- Il NIST deve avviare un progetto pilota di migrazione PQC

Entro 31/12/2030:

- Gli *High Value Assets* devono migrare a PQC per il key establishment

Entro 31/12/2031:

- Gli *High Value Assets* devono migrare a PQC per firma digitale



**Tempi anticipati
rispetto a
precedenti
indicazioni USA**



La Roadmap impone 3 **milestone** fondamentali:

Entro il 31.12.2026



Stabilire Piano Nazionale di transizione

Entro il 31.12.2030



Completare la transizione al PQC per i sistemi ad **alto** rischio

Entro il 31.12.2035



Completare la transizione PQC per i sistemi a **medio** rischio (e il più possibile i sistemi a **basso** rischio)



L'Agenzia ha avviato la redazione del **Piano Nazionale di transizione alla PQC** in coerenza con le tempistiche europee

Scenario e inquadramento normativo



Contesto di riferimento: minaccia quantistica, principi della crittografia post-quantum e il concetto di **crypto-agility**.

Quadro normativo e regolamentare nazionale e internazionale.

Governance nazionale del processo di transizione



Principali **tempistiche di transizione**, modello di coordinamento nazionale, piano di **awareness** e processo di monitoraggio a livello nazionale.

Raccomandazioni tecniche e guide operative



Dettaglio del processo di transizione, raccomandazioni operative ACN a supporto della transizione stessa, includendo tutti i passi che si rendono necessari ad avviare e terminare la transizione.

Raccomandazioni tecniche e guide operative

Struttura organizzativa per la gestione della transizione

Sviluppo di competenze per guidare la transizione

Identificazione asset crittografici

Calcolo del rischio quantistico

Pianificazione delle attività di transizione

➤ **Avvio e monitoraggio delle attività di transizione**

➤ **Linee guida sugli algoritmi da utilizzare**



**Primo semestre
2027**

Transizione alla PQC - Linea di azione nazionale



Pianificazione nazionale	Entro Ottobre 2026	Gruppo di lavoro istituzionale - Principali stakeholder pubblici ed esperti del settore - Prima riunione 17/09, successive con cadenza quindicinale	WORK IN PROGRESS
	Entro Novembre 2026	Coinvolgimento altre istituzioni e settore industriale - Raccogliere osservazioni da parte di altre istituzioni tramite tavoli preesistenti e da rappresentanti e associazioni di categoria	
	Entro Dicembre 2026	Pubblicazione Piano Nazionale di transizione	
	Entro Giugno 2027	Emissione linee guida operative e raccomandazioni sugli algoritmi	
Pianificazione dei soggetti	Entro 2028	Pianificazione attività di transizione da parte dei soggetti interessati	
Esecuzione	Entro 2030	Completamento attività di transizione per sistemi ad alto rischio	
	Entro 2035	Completamento attività di transizione per sistemi a medio e basso rischio	



Avviare subito l'inventario crittografico

Mappare algoritmi, certificati, PKI, firme digitali, VPN, TLS e dipendenze dai fornitori.



Investire nella crypto-agility

Progettare sistemi in grado di sostituire rapidamente algoritmi e componenti crittografici



Valutare il rischio quantistico

Identificare dati e servizi con requisiti di riservatezza a lungo termine, esposti a scenari "*Harvest Now, Decrypt Later*"



Definire governance e competenze

Assegnare responsabilità, sviluppare competenze interne e coinvolgere tempestivamente fornitori e partner.



Pianificare budget e roadmap

Integrare la transizione PQC nei piani di evoluzione tecnologica pluriennali.

La sfida non è scegliere un nuovo algoritmo, ma preparare oggi organizzazioni, processi e infrastrutture per una transizione che durerà anni.



Transizione alla crittografia post-quantum

Alessandro Casale – Capo Divisione algoritmi e applicazioni
crittografiche

Milano,
22.09.2026